PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 12/14, 161/00

A1

(11) International Publication Number: **WO 00/33196**

(43) International Publication Date: 8 June 2000 (08.06.00)

(21) International Application Number: PCT/AU99/01056

(22) International Filing Date: 26 November 1999 (26.11.99)

(30) Priority Data:
PP 7342 26 November 1998 (26.11.98) AU

(71) Applicant *(for all designated States except US)*: ARISTOCRAT LEISURE INDUSTRIES PTY. LTD. [AU/AU]; 71 Longueville Road, Lane Cove, NSW 2066 (AU).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: LYONS, Martin [AU/AU]; 116/362 Mitchell Road, Alexandria, NSW 2015 (AU). MUIR, Robert [AU/AU]; 85–113 Dunning Avenue, Rosebery, NSW 2018 (AU).

(74) Agent: F.B. RICE & CO.; 605 Darling Street, Balmain, NSW 2041 (AU).

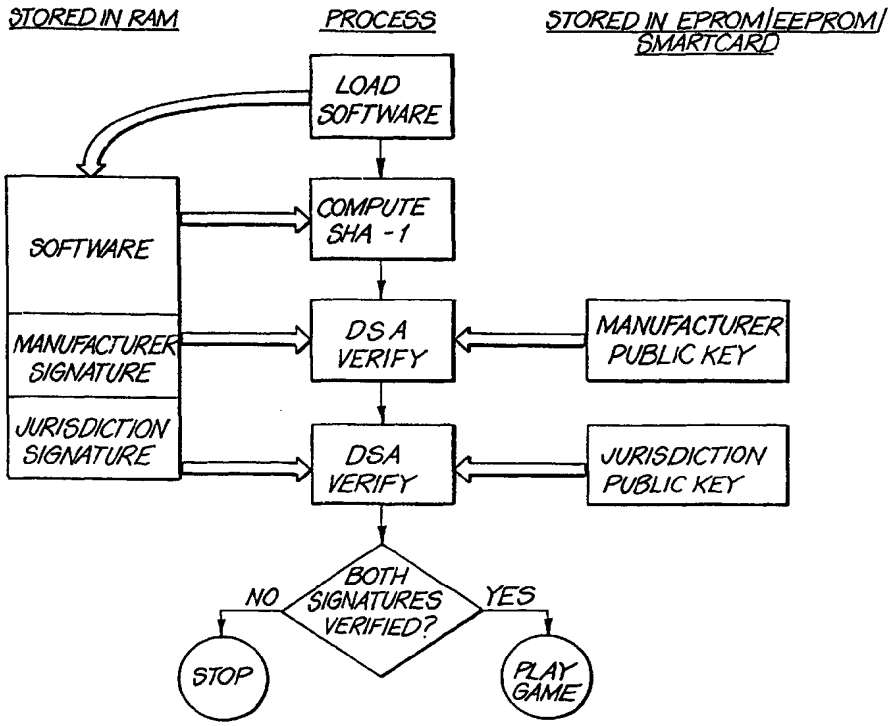
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: ELECTRONIC CASINO GAMING WITH AUTHENTICATION AND IMPROVED SECURITY

(57) Abstract

A gaming machine is described in which all interested parties to a game program to run on the gaming machine, will digitally sign each piece of approved software prior to installation. These signatures are stored with the software on a mass storage device inside the gaming machine. When the machine needs to load a piece of software, or upon an external command after a significant event such as a jackpot payout, it will execute the SHA–1 program code in the EPROM on the software being loaded, and then perform a DSA verification operation using the SHA–1 output as one of the parameters. The DSA verification operation will be repeated for every digital signature stored with the software, and all must be valid, so that it is impossible to execute program code that has not been approved by the manufacturer, the jurisdictional authority and optionally the casino and/or other parties.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Electronic casino gaming with authentication and improved security

Introduction

The present invention relates generally to electronic gaming machines or consoles and in particular the invention provides an improved system for executing casino games in RAM as opposed to the conventional unalterable ROM. The improvements provide an authentication process based upon digital signatures, with the U.S. Digital Signature Standard (DSS) being the preferred means of implementation.

For the sake of clarity the following terms are defined for the purpose of this specification.

A gambling machine, usually referred to as a gaming machine, is a traditional gaming machine. Typical examples include slot machines of the type made by Aristocrat Leisure Industries or IGT.

A casino refers to the operator of gambling machines.

A digital signature is a pair of large numbers represented in a computer as strings of binary digits. The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified.

Strong encryption is the encryption of data such that it is computationally infeasible for a third party - for example a government agency - to retrieve the encrypted data without a key.

A hash, or message digest, is the output from a function that produces a value that is unique for any message input into it. A one-way hash produces an output that is computationally difficult to relate to the input. It is also computationally difficult to produce two different messages with the same message digest.

An unforgeable log is produced by chaining together hash values such that the nth entry in the log is dependent on the (n-1)'h entry, and thus previous entries cannot be altered without re-computing the whole chain.

A logic cage is a secure area inside the gaming machine that cannot be accessed without sufficient security clearance.

References

"The Digital Signature Standard" U.S. Federal Information Processing Standards Publication 186

"The Secure Hash Standard" U.S. Federal Information Processing Standards Publication 180-1

"Cryptographic Support for Secure Logs on Untrusted Machines" by Bruce Schneier and John Kelsey (available at http://www.counterpane.com/secure-logs. html)

Background of the Invention

Traditionally, microprocessor based gaming machines store their program contents in unalterable ROM or EPROM. During installation and after a large jackpot payout, the machine is physically inspected and the EPROMs are removed. These EPROMs are placed in a verification device which produces an output string using a known algorithm usually referred to as a hash function. This string is compared against a string that has been already generated when the game software was approved by the gaming jurisdiction. Authentication is achieved by a match of the approved string and the EPROM generated string.

The main disadvantage of such a system is that the current limited capacity of EPROM technology ensures that games cannot be as sophisticated as if they were stored in an alternative medium such as a hard disk or CD-ROM. The other problem with using RAM is that it cannot be extracted and placed in a verification device, since the contents of the RAM are necessarily volatile.

Another system, disclosed and described in U.S. Pat. No. 5,643,086 uses a private key to encrypt a message digest of the approved copy of the software, and thus produce an unalterable digital signature which can be decrypted with a corresponding public key and compared against a message digest generated by an unalterable EPROM in the gaming machine.

The disadvantage of the above invention is that it relies on strong encryption, currently subject to export restrictions from the U.S. and other countries. This software can only be signed by one party and if a single private key is compromised, the whole system is compromised.

A related problem that exists is that of version control. Once a gaming machine software program is found to be faulty, a modification or 'patch' is usually distributed. Unfortunately, conventional EPROM based machines, and the disclosed system above, have no method implemented of ensuring that the earlier version of the software is not re-installed, either deliberately or by accident, later. Once software is approved, it is impossible for the machine to revoke that approval. If a rogue element was able to 'sneak past' a

jurisdiction a dubious piece of software, there would be no way to stop it being used in a casino, even after detection

Summary of the Invention

The invention provides a gaming machine with enhanced capability for storing games due to enhanced security and authentication capabilities.

According to a first aspect the present invention provides a programmable controller, including a readable and writable storage means to hold a program during its execution by the programmable controller, and program authentication means comprising digital signature verification means which verifies a digital signature associated with the program and prevents execution of the program if the digital signature is not valid.

According to a second aspect the present invention provides a method of verifying a program or a program component for a programmable controller, including a readable and writable storage means to hold a program during its execution by the programmable controller, and program authentication means comprising digital signature verification means which verifies a digital signature associated with the program, and the method including a step of verifying the digital signature against a key, and preventing execution of the program if the digital signature is not valid.

Preferably, the digital signature is generated by a method that does not include encryption such that de-encryption is not performed during the digital signature verification.

According to a third aspect the present invention provides a programmable controller, including a readable and writable storage means to hold a program during its execution by the programmable controller, and program authentication means comprising digital signature verification means which verifies each of a plurality of digital signatures associated with the program and prevents execution of the program if any one of the digital signatures is not valid.

According to a fourth aspect the present invention provides a method of verifying a program or a program component for a programmable controller, including a readable and writable storage means to hold a program during its execution by the programmable controller, and program authentication means comprising digital signature verification means which verifies each of a plurality of digital signatures associated with the program, and the method including steps of verifying each of the digital signatures

against a respective key, and preventing execution of the program if any one of the digital signatures is not valid.

Preferably the or each digital signature is generated by a method that does not include encryption such that de-encryption is not performed during the digital signature verification.

In one embodiment, the programmable controller is used to control the operation of a game played on an electronic gaming machine and the signed program is a game program or a component of a game program.

Preferably multiple signatures may be applied to the game software, to ensure that only software approved by not only the manufacturer, but also the jurisdictional authority and optionally the casino itself, is executed by the machine

Preferably also a system is provided for revoking signature keys. This can be password based - a password is entered which allows one of the public signatures stored in the machine to be changed. Alternatively, a revocation certificate can be used, which must be valid, or the revocation system can be time based, where the machine stores a set of signatures, good for say 10 years, and the current active signature is based upon the current system clock.

A system of equivalent signatures is also preferably provided, such that any one of these signatures can be used as part of the verification. Ideally a manufacturer will have at least one signature for its office in each jurisdiction. Any one could be used to sign a game, but it would be apparent in the event of a problem where the responsibility would lie, and could be revoked easily.

Preferably a system for version control is also included, such that once a later version of software runs on a gaming machine it is then impossible to run an earlier version of the same software. This would preferably permanently revoke faulty games once a fix had been issued.

Preferably any signature and version changes are held in secure unforgeable logs updated after each change to help detect possible fraud. Preferably also the unforgeable logs are implemented using tamper-proof devices such as smartcards to ensure that the log can never be deleted.

Brief Description of the Drawings

Embodiments of the present invention will now be described by way of example with reference to the accompanying drawings in which:

Figure 1 illustrates a conventional gaming machine in which the present invention may be implemented;

Figure 2 is a block diagram of a control unit according to the present invention;

Figure 3 is a diagrammatic representation of a method of signature generation and verification according to the present invention;

Figure 4 is a flow diagram of a software approval process according to the present invention; and

Figure 5 is a flow diagram illustrating a method of executing approved software according to the present invention.

Detailed Description of the preferred embodiments

In the following detailed description the methodology of the embodiments will be described, and it is to be understood that it is within the capabilities of the non-inventive worker in the art to introduce the methodology on any standard microprocessor-based gaming machine or gaming console by means of appropriate programming.

Referring to Figure 1 of the drawings, the first embodiment of the invention is illustrated in which a slot machine 40, of the type having a video display screen 41 which displays a plurality of rotatable reels 42 carrying symbols 43, is arranged to pay a prize on the occurrence of a predetermined symbol or combination of symbols.

In the slot machine 40 illustrated in Figure 1, the game is initiated by a push button 44, however, it will be recognized by persons skilled in the art that this operating mechanism might be replaced by a pull handle or other type of actuator in other embodiments of the invention. The top box 45 on top of the slot machine 40 carries the artwork panel 35 which displays the various winning combinations for which a prize is paid on this machine.

The program which implements the game and user interface is run on a standard gaming machine control processor 100 as illustrated schematically in Figure 2. This processor forms part of a controller 110 which drives the video display screen 141 and receives input signals from sensors 144. The sensors 144 may be touch sensors, however, in alternative embodiments these may be replaced by a pull handle or another type of actuator such as

button 44 in Figure 1. The controller 110 also receives input pulses from a mechanism 120 indicating the user has provided sufficient credit to begin playing. The mechanism 120 may be a coin input chute, a bank note acceptor (bill acceptor), a credit card reader, or other type of validation device. The controller 120 also drives a payout mechanism 130 which for example may be a coin output.

The controller 110 also includes ROM 170 in which fixed and secure program components are held. This ROM may also contain part or all of a program to perform a program verification function for programs running on the CPU 100 out of RAM 150 or loaded onto or from the disk 160.

Alternatively, the program verification may be performed by a stand alone verification system 140 interposed between the RAM 150, the disk 160 and the CPU 100. The verification system may make use of a tamper proof storage element such as a smart card 180 (or a device containing a smart card chip, or the verification system 140 may itself be implemented as a smart card or smart card chip in which case, it will not require the separate smart card 180. An Input/Output function 190 is also provided for the CPU to communicate with a gaming machine network for administration participation in system wide prizes and bonuses and for downloading of game programs.

The game played on the machine shown in Figures 1 and 2 is a relatively standard game which includes a 3 by 5 symbol display and allows multiple pay lines.

Slot machines such as those of the type described with reference to Figures 1 and 2 can be adapted to embody the present invention with generally only a software change to modify the functions of some of the user interfaces of the machine.

The system, when built will consist of an electronic gaming machine, with standard features such as graphics capability, a monitor, sound output and interfaces to gaming hardware such as hoppers, bill acceptors etc. The gaming machine would also have a sophisticated central processor, say a Pentium or PowerPC for example, with a large amount of RAM, a storage device such as a hard disk, CD-ROM or remote network storage and optionally a smartcard interface.

The machine would furthermore have an unalterable EPROM which would have stored in it program code to perform the DSS algorithm, also

know as the DSA. It would also contain code to perform the Secure Hash Algorithm (SHA-1), the designated U.S. Federal standard message digest algorithm. This EPROM would be able to be extracted and inspected by the traditional means. In alternative implementations, other digital signature algorithms could be used such as GOST, ESIGN or even the previously disclosed RSA method which requires encryption.

Figure 3, copied from the U.S. Federal standard FIPS 180-1, describes the operations that produce and verify a digital signature using DSA and SHA-1. An important distinguishing characteristic of this system is that it does not use encryption to produce a digital signature. It is thus not subject to export restrictions from the US and other countries.

Each set of software that is to be installed in any gaming machine at present must be approved, both by the gaming jurisdictional authority and by the machine manufacturer. It also may need to be approved by the casino in which the machine will reside. In the preferred implementation, all interested parties will digitally sign each piece of approved software prior to installation. The process of game software being produced, approved and authenticated would proceed as in Figure 4.

These signatures will be stored with the software on a mass storage device inside the gaming machine. When the machine needs to load a piece of software, or upon an external command after a significant event such as a jackpot payout, it will execute the SHA-1 program code in the EPROM on the software being loaded, and then perform a DSA verification operation using the SHA-1 output as one of the parameters. The DSA verification operation will be repeated for every digital signature stored with the software, and all must be valid, so that it is impossible to execute program code that has not been approved by the manufacturer, the jurisdictional authority and optionally the casino and/or other parties. The process of executing pre-approved software would proceed as in Figure 5.

A significant benefit of multiple signatures, as opposed to other disclosed systems which use only one, is that it protects all parties from a rogue element working within either the manufacturer, the jurisdiction or the casino. To successfully install a fraudulent piece of software in a gaming machine that uses this system would require a concerted conspiracy involving trusted personnel working for all parties.

To perform the digital signature verification, it is also necessary that the machine store public keys for the appropriate parties - jurisdiction, casino and manufacturer. In the preferred implementation, these keys are stored in EEPROM, which can be modified at suitable times by a program stored in the EPROM, under strict security conditions. This enables signatures to be revoked if compromised, or periodically updated. In an alternative implementation, a plurality of signature public keys are stored in the unalterable EPROM and variables stored in EEPROM indicate which of these signatures are active. In another alternative implementation, a tamper-proof device such as a smartcard stores the public keys. The program code in the EPROM passes the output from the SHA-1 algorithm to the smartcard along with the signature values stored with the software. The smartcard then performs the DSS or other signature verification and returns either an authentication or denial code to the gaming machine. Once revoked, the smartcard will not allow keys to be re-enabled.

Since it will be possible to change the digital signatures that authenticate software running in the machine, it is important that an unforgeable log is kept of all software changes or signature changes. This can be achieved by the use of a hash chain, where every entry in the log is 'hashed' with the previous log entry's hash value. In a preferred implementation, this hash chain, or the most recent part of it, is stored within a tamper-proof device such as a smartcard or the traditionally used logic cage. A smartcard is preferred, since it can have a secret, unique identification code, and is thus non-reproducible and unforgeable itself. Program code stored in the unalterable EPROM accesses the smartcard during signature or software update. Since the latest hash value would always be stored on the smartcard, it would be impossible to change the software without creating a log entry. This would ensure that all modifications to the software stored on the machine was accurately logged which L would be extremely useful in the event of a major jackpot payout. The EPROM can be proven to be unaltered by I the conventional means of placing it in a verification device.

A more detailed description of a possible implementation of a hash-chain unforgeable log can be found in the paper "Cryptographic Support for Secure Logs on Untrusted Machines" - see references above.

Each signature for a file would be linked to the file, but need not be contained within the file. In the event of a signature key revocation, new signatures may have to be downloaded from a network device or using the machine's operator mode. In this case. the new signatures being downloaded would indicate which file they are to attach to, and which signature they replace. This would be more economical than re-downloading the whole software set upon a signature key change.

In an alternative implementation, multiple public keys for each corresponding signature are stored. At any one time, only one for each interested party would be active. The schedule for selecting which public keys are active could be time-based, so signatures would in effect have a lifetime. Periodically, the machine would have to be updated with the new signatures as either a maintenance task or upon the payments of an additional license fee to the manufacturer or jurisdiction.

In the event of an authentication failure due to signatures (and therefore the license to run the software) expiring, it could be implemented that the casino would have a 'grace' period to obtain new keys before the machine completely refused to run the software. For example, the machine could display a notice, similar to that found on computer shareware products, informing of the license expiry that would have to be manually accepted by the machine operator every time the machine was reset.

In the alternative implementation, it would also be possible to have multiple signatures active for each party at any one time. One possibility would be that these would correspond to different divisions within the manufacturer or jurisdiction. This would aid tracing in the event of a software or security failure.

Another security aspect that will be implemented in the gaming machine is the concept of version control. Each digitally signed piece of software stored on the mass storage device within the machine will have an associated identification code and version number. It will be impossible to download software with a corresponding identification code and an earlier version number.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS

1. A programmable controller, including a readable and writable storage means to hold a program during its execution by the programmable controller, and program authentication means comprising digital signature verification means which verifies a digital signature associated with the program and prevents execution of the program if the digital signature is not valid, the digital signature being generated by a method that does not include encryption such that de-encryption is not performed during the digital signature verification.

2. The controller as claimed in claim 1, wherein a plurality of signatures are applied to the game software.

3. A programmable controller, including a readable and writable storage means to hold a program during its execution by the programmable controller, and program authentication means comprising digital signature verification means which verifies each of a plurality of digital signatures associated with the program and prevents execution of the program if any one of the digital signatures is not valid.

4 The electronic gaming machine as claimed in claim 2 or 3, wherein one of the digital signatures is applied to the software by or on behalf of a manufacturer of the electronic gaming machine.

5. The controller as claimed in claim 2, 3 or 4, wherein one of the digital signatures is applied to the software by or on behalf of a jurisdictional authority that has jurisdiction to authorize use of the game in a location in which the game is installed.

6. The controller as claimed in claim 2, 3, 4 or 5, wherein one of the digital signatures is applied to the software by or on behalf of a casino in which the electronic gaming machine is installed.

7. The controller as claimed in any one of claims 1 to 6, wherein the programmable controller is used to control the operation of a game played on an electronic gaming machine and the program with which the digital signature is associated is a game program or a component of a game program.

8. The controller as claimed in any one of claims 1 to 7, wherein the signature verification means stores one or more public signature keys in secure storage and uses a public signature key from the secure storage to verify the digital signature associated with the game program.

9. The controller as claimed in claim 8, wherein the signature verification means includes signature revocation means for removing public signature keys from a set of valid keys as a method of revoking signature keys.

10. The controller as claimed in claim 9, wherein the signature revocation means is activated by a password such that when the password is entered it allows a particular public signature stored in the verification means to be changed or deleted.

11. The controller as claimed in claim 9 or 10, wherein a digital revocation certificate can be used, which must be validated by the validation means before it causes a public signature key to be revoked.

12. The controller as claimed in claim 9, 10 or 11, wherein revocation is time based, whereby the machine stores a set of public signature keys, which are valid for a fixed period of time, after which they are automatically revoked.

13. The controller as claimed in claim 12, wherein the fixed period before automatic revocation is a period of 10 years.

14. The controller as claimed in claim 12 or 13, wherein identification of a current active public signature is based upon comparison of a time stamp embedded in the signature with a time and date obtained from a current time value from a system clock.

15. The controller as claimed in any one of claims 8 to 14, wherein a plurality of equivalent signatures are provided in the secure storage, such that any one of the equivalent signatures can be used as part of the verification authorization.

16. The controller as claimed in claim 15, wherein each of the equivalent signatures is identifiable as being associated with a person or entity responsible for issuing or authorizing the program

17. The controller as claimed in any one of claims 1 to 16, wherein the verification program records versions of a program that have been verified and will not re-verify versions earlier than the latest version that it has already verified.

18. The controller as claimed in claim 17, wherein the record of verified program versions is stored in a secure log and entries in the record are unforgable and unalterable after being written.

19. The controller as claimed in claim 18, wherein a record of digital signature key updates is kept in the secure log.

20. The controller as claimed in claim 18 or 19, wherein the secure log is recorded in a tamper proof device.

21 The controller as claimed in claim 20, wherein the tamper proof device is a smartcard or contains a smartcard chip.

22. A method of verifying a program or a program component for a programmable controller, including a readable and writable storage means to hold a program during its execution by the programmable controller, and program authentication means comprising digital signature verification means which verifies a digital signature associated with the program, the digital signature being generated by a method that does not include encryption and the method including a step of verifying the digital signature against a key, in which de-encryption is not performed during the digital signature verification, and preventing execution of the program if the digital signature is not valid.

23. The method as claimed in claim 22, a plurality of signatures are applied to the game software.

24. A method of verifying a program or a program component for a programmable controller, including a readable and writable storage means to hold a program during its execution by the programmable controller, and program authentication means comprising digital signature verification means which verifies each of a plurality of digital signatures associated with the program, and the method including steps of verifying each of the digital signatures against a respective key, and preventing execution of the program if any one of the the digital signatures is not valid.

25. The method as claimed in claim 23 or 24, wherein one of the digital signatures is applied to the software by or on behalf of a manufacturer of the electronic gaming machine.

26. The method as claimed in claim 23 or 24 or 25, wherein one of the digital signatures is applied to the software by or on behalf of a jurisdictional authority that has jurisdiction to authorize use of the game in a location in which the game is installed.

27. The method as claimed in claim 23 or 24 or 25 or 26, wherein one of the digital signatures is applied to the software by or on behalf of a casino in which the electronic gaming machine is installed.

28. The method as claimed in any one of claims 22 to 27, wherein the programmable controller is used to control the operation of a game played on

an electronic gaming machine and the program with which the digital signature is associated is a game program or a component of a game program.

29. The method as claimed in any one of claims 22 to 28, wherein the signature verification means stores one or more public signature keys in secure storage and uses a public signature key from the secure storage to verify the digital signature associated with the game program.

30. The method as claimed in claim 29, wherein the signature verification means includes signature revocation means for removing public signature keys from a set of valid keys as a method of revoking signature keys.

31. The method as claimed in claim 30, wherein the signature revocation means is activated by a password such that when the password is entered it allows a particular public signature stored in the verification means to be changed or deleted.

32. The method as claimed in claim 30 or 31, wherein a digital revocation certificate can be used, which must be validated by the validation means before it causes a public signature key to be revoked.

33. The method as claimed in claim 30, 31 or 32, wherein revocation is time based, whereby the machine stores a set of public signature keys, which are valid for a fixed period of time, after which they are automatically revoked.

34. The method as claimed in claim 33, wherein the fixed period before automatic revocation is a period of 10 years.

35. The method as claimed in claim 33 or 34, wherein identification of a current active public signature is based upon comparison of a time stamp embedded in the signature with a time and date obtained from a current time value from a system clock.

36. The method as claimed in any one of claims 29 to 35, wherein a plurality of equivalent signatures are provided in the secure storage, such that any one of the equivalent signatures can be used as part of the verification.

37. The method as claimed in claim 36, wherein each of the equivalent signatures is identifiable as being associated with a person or entity responsible for issuing or authorizing the program.

38. The method as claimed in any one of claims 22 to 37, wherein the verification program records versions of a program that have been verified

and will not re-verify versions earlier than the latest version that it has already verified

39. The method as claimed in claim 38, wherein the record of verified program versions is stored in a secure log and entries in the record are unforgable and unalterable after being written.

40. The method as claimed in claim 39, wherein a record of digital signature key updates is kept in the secure log.

41. The method as claimed in claim 39 or 40, wherein the secure log is recorded in a tamper proof device.

42. The method as claimed in claim 41, wherein the tamper proof device is a smartcard or contains a smartcard chip.

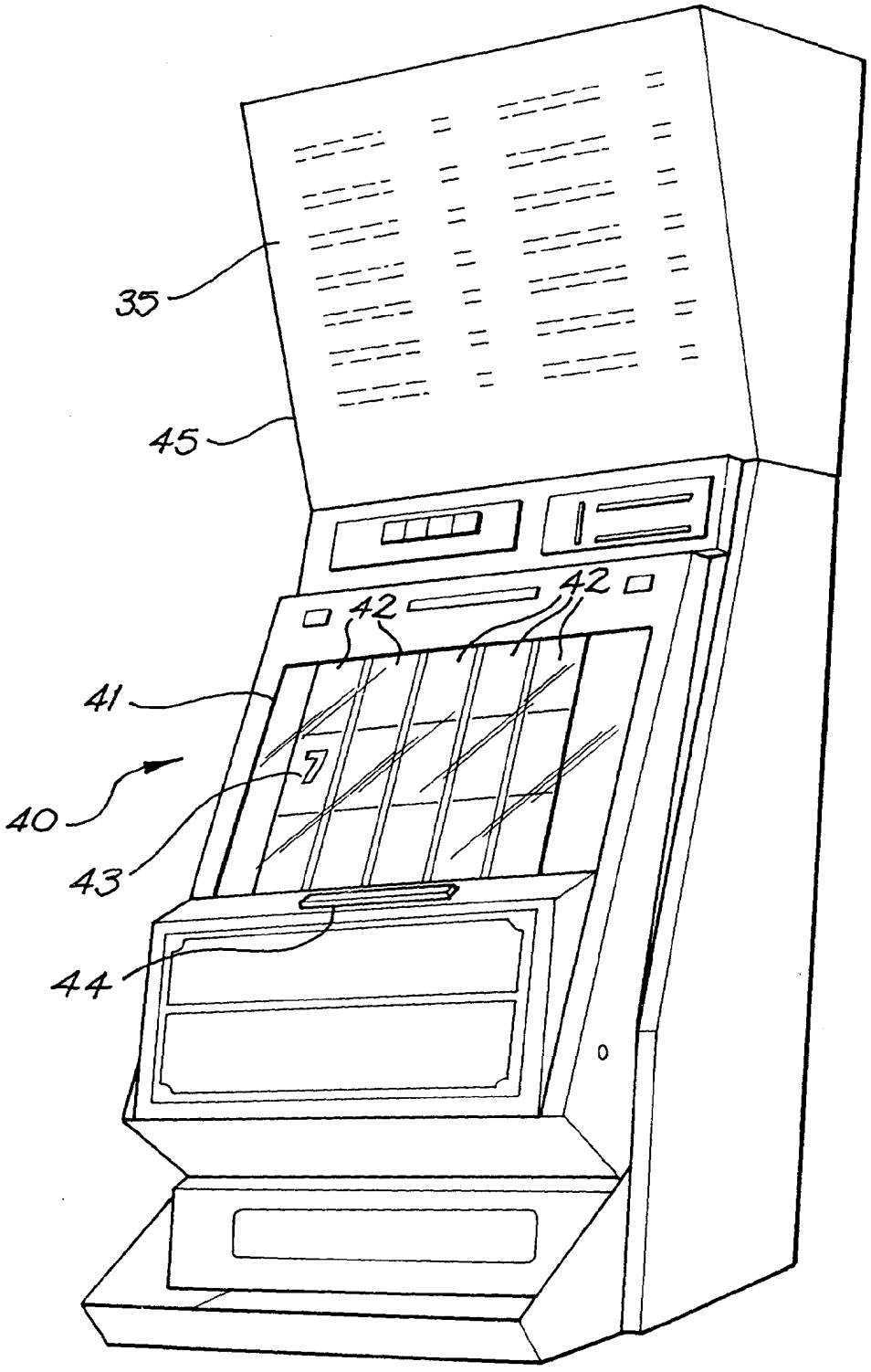


FIG. 1

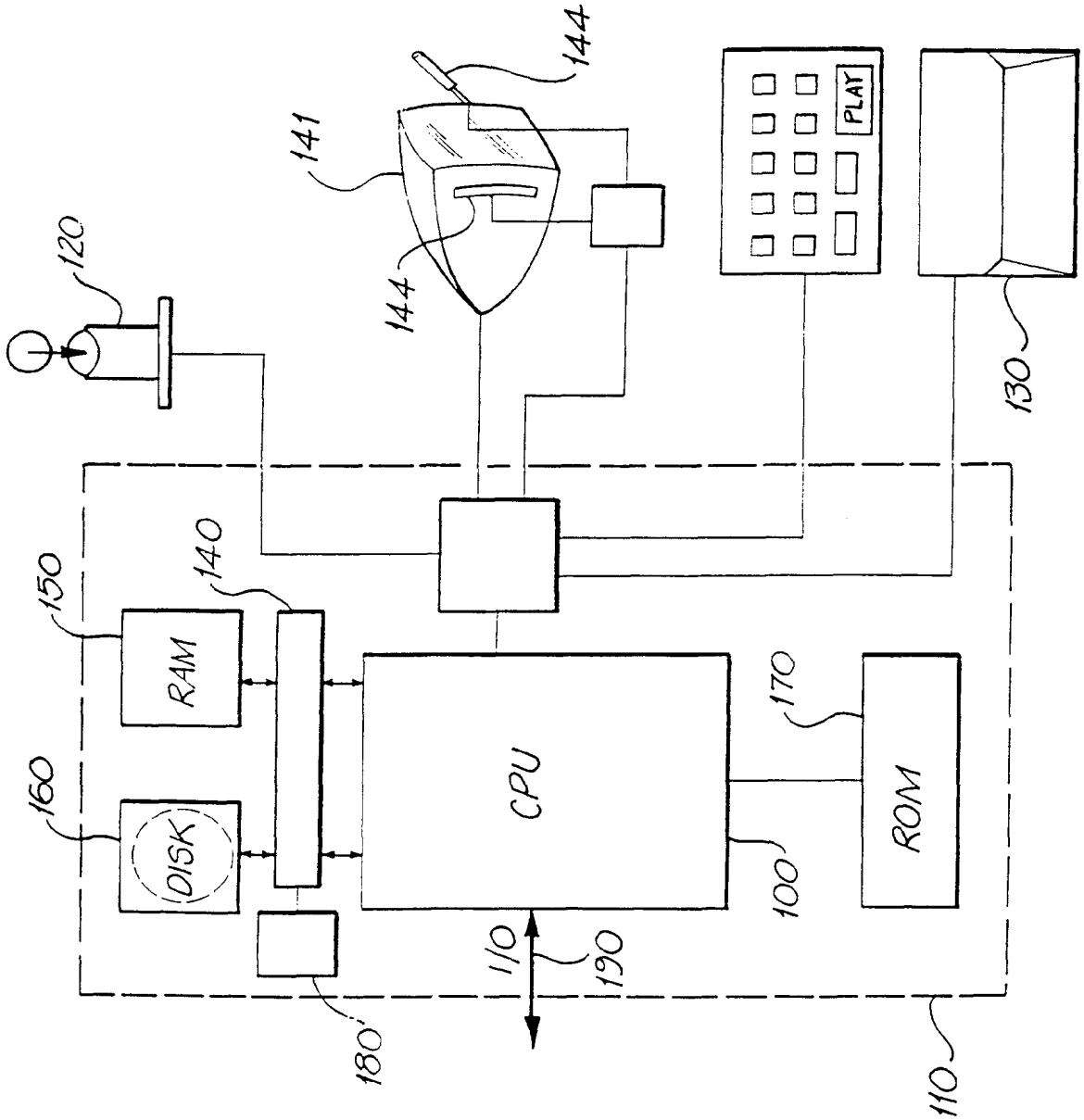

120
141
144
144
PLAY
130
150
140
RAM
160
DISK
CPU
170
ROM
100
110
190
180

FIG. 2

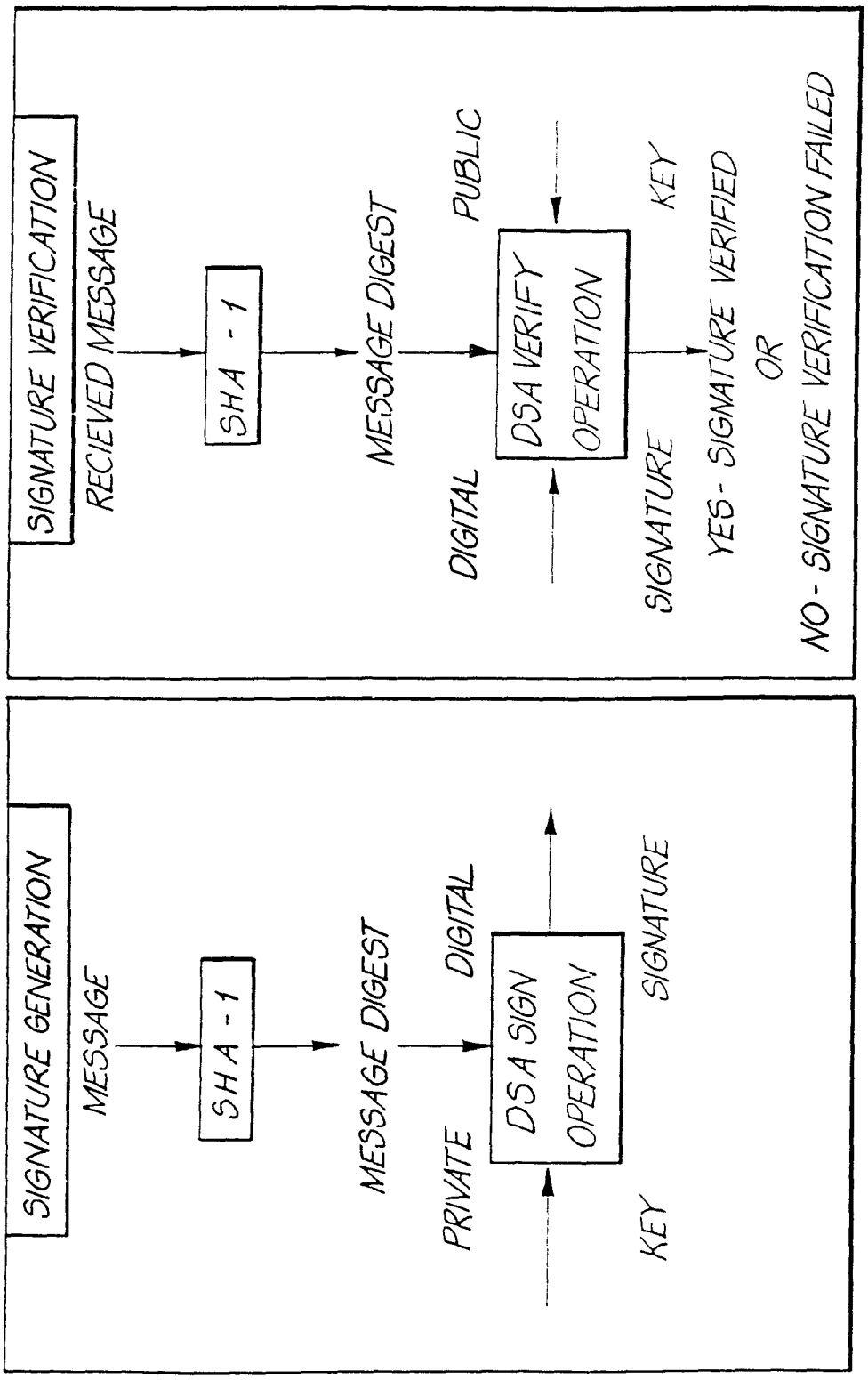

SIGNATURE GENERATION
MESSAGE
SHA - 1
MESSAGE DIGEST
DIGITAL
PRIVATE
DSA SIGN OPERATION
KEY
SIGNATURE
SIGNATURE VERIFICATION
RECIEVED MESSAGE
SHA - 1
MESSAGE DIGEST
PUBLIC
DIGITAL
DSA VERIFY OPERATION
KEY
SIGNATURE
YES - SIGNATURE VERIFIED
OR
NO - SIGNATURE VERIFICATION FAILED

FIG. 3

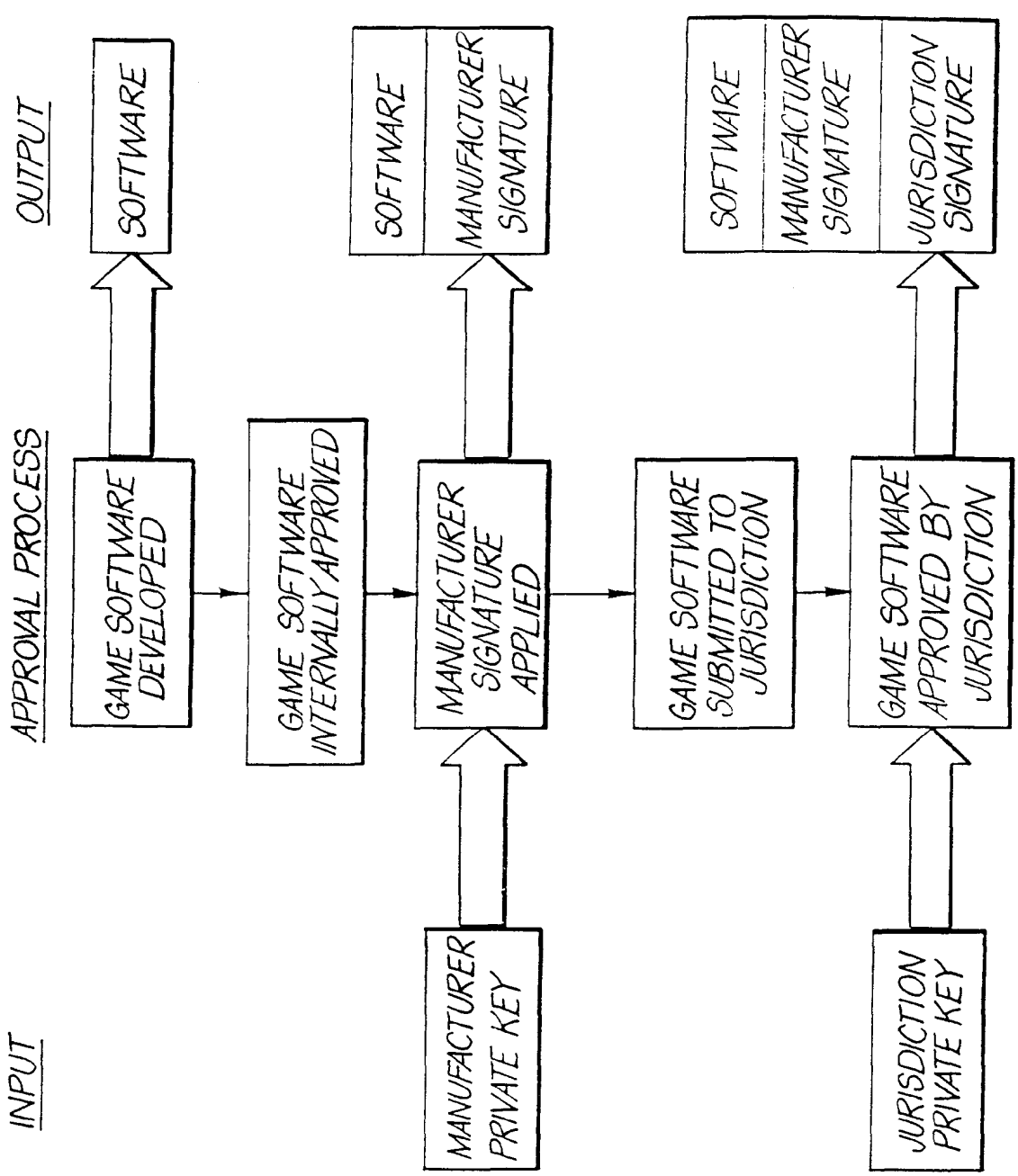

APPROVAL PROCESS
INPUT
OUTPUT
GAME SOFTWARE DEVELOPED
SOFTWARE
GAME SOFTWARE INTERNALLY APPROVED
MANUFACTURER SIGNATURE APPLIED
MANUFACTURER PRIVATE KEY
SOFTWARE
MANUFACTURER SIGNATURE
GAME SOFTWARE SUBMITTED TO JURISDICTION
GAME SOFTWARE APPROVED BY JURISDICTION
JURISDICTION PRIVATE KEY
SOFTWARE
MANUFACTURER SIGNATURE
JURISDICTION SIGNATURE

FIG. 4

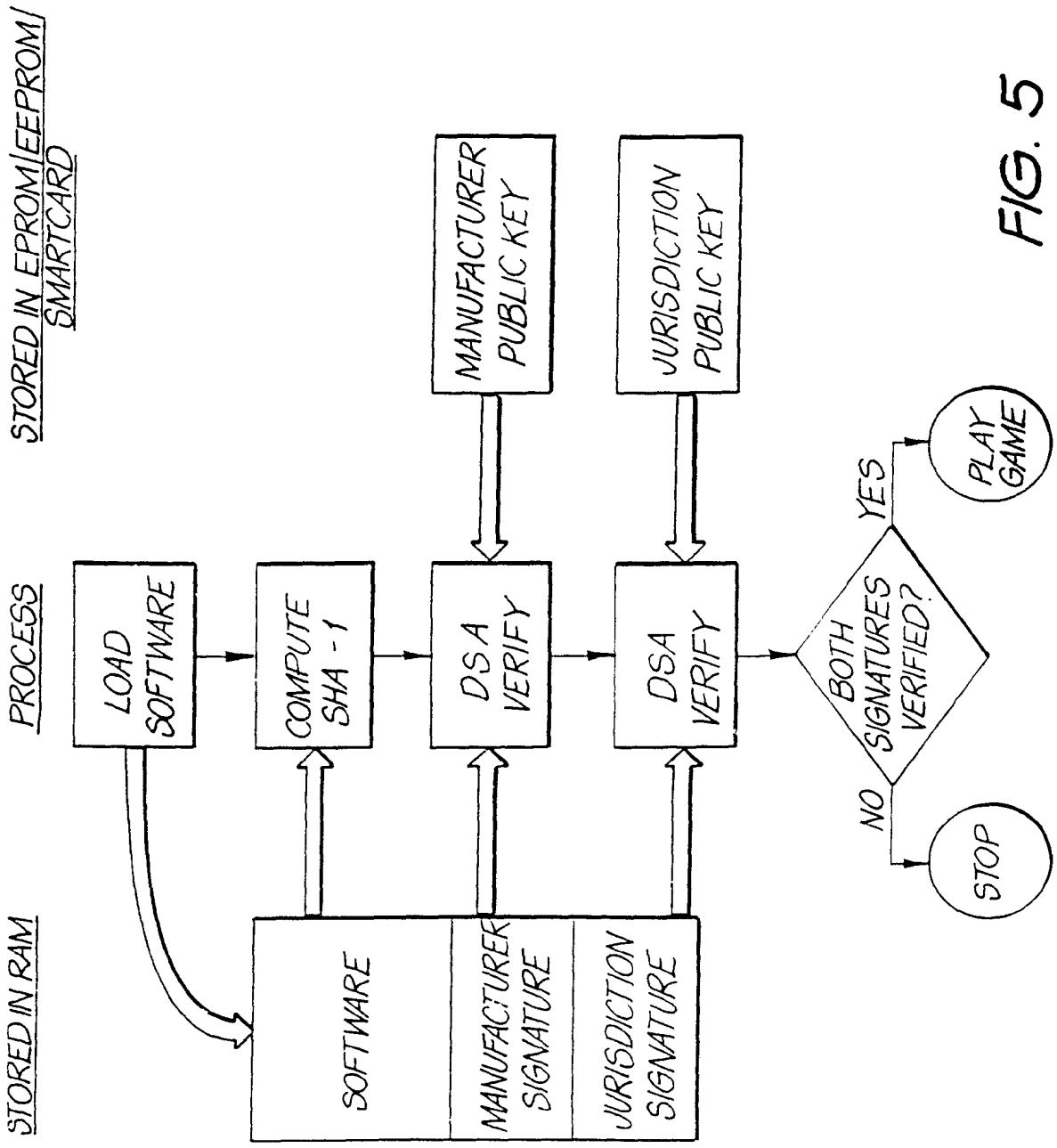

STORED IN EPROM/EEPROM/ SMARTCARD
PROCESS
STORED IN RAM
LOAD SOFTWARE
COMPUTE SHA - 1
DSA VERIFY
DSA VERIFY
MANUFACTURER PUBLIC KEY
JURISDICTION PUBLIC KEY
BOTH SIGNATURES VERIFIED?
YES
NO
PLAY GAME
STOP
SOFTWARE
MANUFACTURER SIGNATURE
JURISDICTION SIGNATURE

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU 99/01056

A. CLASSIFICATION OF SUBJECT MATTER

Int Cl[6]: G06F 12/14, 161/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC G06F12/-, 19/-, A63F 9/24, 9/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
AU:IPC AS ABOVE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT, JAPIO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5638447A, MICALI, 10 June 1997, whole document	1,3,8,22,24,29
X	JP 09251268A, MATSUSHITA ELECTRIC IND CO LTD, 22 September 1997,abstract	3,24
A	US 5778070A, MATTISON, 7 July 1998	

[X] Further documents are listed in the continuation of Box C

[X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 December 1999	30 DEC 1999
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	**S KAUL** Telephone No.: (02) 6283 2182

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU 99/01056

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5421006A, JABLON et al, 30 May 1995	
A	US 5721781A, DEO et al, 24 February 1998	

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU 99/01056

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	5778070	AU	36448/97	CN	1229513	GB	2330228
		WO	9800846				